Journal of Autonomous Intelligence (2024) Volume 7 Issue 5
doi: 10.32629/jai.v7i5.1488

ORIGINAL RESEARCH ARTICLE

Performance optimization of multipath K-AOMDV protocol using SVM against blackhole attack

Sheetal Kaushik[1,*], Khushboo Tripathi[2], Rashmi Gupta[2], Prerna Mahajan[3]

[1] *Amity School of Engineering and Technology, Gurugram 122413, Haryana, India*

[2] *Department of Computer Science and Engineering, Amity school of Engineering and Technology, Amity University Haryana, Gurugram 122413, India*

[3] *IITM Janakpuri, New Delhi 110058, India*

*** Corresponding author:** Sheetal Kaushik, Sheetal.kaushik618@gmail.com

ABSTRACT

This research focuses on the Ad Hoc On-Demand Multi-Path Routing (AOMDV) protocol, which is preferred for its improved efficiency compared to a single-path routing protocol in mobile ad hoc networks (MANETs). However, identifying attackers in such networks is a complicated task due to malicious nodes providing optimistic, forward-looking optimistic responses. In this study, the author proposes a novel security solution, the K-AOMDV (KNN- Ad Hoc On-Demand Multi-Path Routing protocol) that uses K-means clustering to prevent routing misbehaviour. The efficiency of the proposed K-AOMDV routing protocol is analyzed using supervised machine learning approach to predict optimal routes with minimal packet hops between nodes. The proposed algorithm has a high accuracy rate of 0.99%, 80% true positives, and 80% recall. It communicates the black hole attacker's node identification (ID) into the network, ensuring that the attacker will not participate in the routing method in the future. The privacy domain in MANET is the main focus of this research, and the proposed solution affiliates an effective approach to enhancing the security of MANETs.

Keywords: K-AOMDV; blackhole attack; MANET; reinforcement learning; SVM; K-NN

ARTICLE INFO

Received: 15 December 2023
Accepted: 29 January 2024
Available online: 21 March 2024

1. Introduction

MANETs have gained considerable emphasis from researchers since the mid-1990s due to their ability to provide advanced wireless communication between mobile nodes, even when there is no permanent infrastructure available. This makes MANETs ideal for scenarios where traditional networks are not feasible including disaster-hit areas or in military operations. The design of a MANET is constantly evolving due to the nodes in the network being able to operate in any direction and at any time to establish and maintain their connections. The dynamic nature of MANETs, along with their decentralized and self-organizing properties, present unique challenges and opportunities for researchers to explore new techniques for routing, security, and performance optimization[1].

A MANET is a wireless network made up of mobile nodes that can communicate with one another in the absence of centralized control or established infrastructure. Nodes can communicate with each other when they are within radio range, and packets are forwarded to nodes that are further away based on the nodes in their direct proximity. Each node in a MANET can act as a host or a router, and mobility is one of the benefits of wireless communication, allowing nodes to move easily

within the network while maintaining connectivity. Compared to wired networks, ad hoc networks offer more flexibility, as nodes can join or leave the network with greater ease. These networks can be utilized in disaster management, battlefields, and remote locations where it is not feasible to install and operate a fixed network. MANETs can also be useful in situations where the construction phase is challenging, making them an attractive option for various applications. For example, MANETs can assist in deploying and coordinating drones on the battlefield[2].

A blackhole attack is a significant threat to the security of these networks, and it can severely disrupt connections between network nodes. The attack involves a malicious node broadcasting a fraudulent route reply in response to a legitimate route request, falsely claiming to have the shortest path without even checking its routing database, which confirms the shortest path, and this attack is called a "route request simulation attack". The Multipath K-AOMDV protocol is an extension of the AOMDV protocol, which uses multiple backward paths between intermediate and final nodes to construct multiple forward paths to the destination. This approach aims to reduce the overhead caused by exploring alternative routes and enhance network efficiency. However, maintaining fields such as Successor Forwarding Routing Pointers (SFRPs), Path Approvals (PAs), and Path Errors (DOPEs) in routing control packets results in additional overhead compared to the AODV protocol[3].

To address this issue, the AOMDV routing protocol includes safeguards against blackhole attacks and other security threats to ensure secure and reliable data transmission between nodes. However, these safeguards may not be sufficient in all cases, and performance optimization of the protocol using SVM against black hole attacks is an effective preventive measure. The Multipath K-AOMDV protocol can then use this classification to route packets through only legitimate nodes, avoiding malicious nodes altogether. By using this approach, the protocol can identify and avoid malicious nodes, ensuring that packets are routed through only legitimate nodes, thereby reducing the risk of network disruption and data loss due to black hole attacks[4].

The AOMDV protocol is commonly used in wireless ad-hoc networks as a reactive protocol for multi-path routing. The proposed approach employs a supervised machine learning model, to enhance the efficiency and reliability of the routing protocol by predicting optimal routes based on available data. The aim is to reduce the number of packet hops required for data transmission between nodes, thereby reducing delay, packet loss, and energy consumption in the network. The Multipath K-AOMDV protocol is an advancement of AOMDV protocol, which uses multiple backward paths between intermediate and final nodes to construct multiple forward paths to the destination in order to reduce the overhead caused by exploring alternative routes and enhance network efficiency.

2. Literature review

Review focuses on the blackhole attacks in MANETs and the reliability of the multi-path K-AOMDV routing protocol. Various researchers have conducted studies to provide a deeper understanding of these issues.

Bhardwaj et al.[5] used clustering methods affected by the insect-lion chase to optimize the effectiveness of research on wireless sensor networks. The authors used three clustering methods affected by the insect-lion chase to optimize the effectiveness of this research. The model's performance is assessed by comparing its findings to those obtained using more conventional approaches.

Abdan et al.[6] examined blackhole attacks and utilized machine learning techniques such as LDA, Decision Trees , Naive Bayes , KNN, SVM, and Convolutional Neural Networks for classification. Decision Tree was found to be the most accurate method with a 98.9% classification rate.

Sivanesan et al.[7] identified wormhole attacks (WHA) as the most dangerous and prevalent among the various types of attacks in MANETs. Existing WHA detection methods require additional resources to

implement. Therefore, the author explored the ML techniques for WHA detection in ad hoc networks. They used SVM and achieved excellent results.

Alsarhan et al.[8] highlights SVM for intrusion detection in vehicular ad hoc networks. To enhance the SVM classifier's accuracy, three artificial intelligence optimization methods were used with Comparative tests indicate that GA outperforms from rest methods.

Rajendran et al.[9] discussed the challenges of developing complex defense schemes in ad hoc networks due to their characteristic and many of these network's detection systems learn from each other's collective routing expertise through supervised learning. A deep learning approach is the best way to address ad hoc network issues.

Chen et al.[10] explored the use of multi-agent reinforcement learning for packet network routing, with the goal of predicting how the policies of neighboring nodes and the traffic volume on the network would affect the nodes. The researchers introduced two advanced model-free multi-agent RL algorithms, namely Multi-agent Proximal Policy Optimization and meta-MAPPO, which aimed to enhance network efficiency in the face of unpredictable traffic levels.

Guo et al.[11] implemented a routing system to determine the most efficient route for data delivery. They developed a reward function that considered factors such as overall energy consumption, stable energy consumption, and the number of hops. The proposed method outperformed in terms of the average energy consumption and PDR.

Kaushik et al.[12] proposes an SVM-based approach for optimizing the performance of multipath K-AOMDV protocol against blackhole attack by comparing SAODV and AODV protocols w.r.t. parameters such as PDR, E-E delay and throughput.

Kaushik et al.[13] explores the application of ML models with different protocols in wireless ad-hoc networks, aiming to enhance performance parameters and optimize quality of service, while studying simulators and evaluating their effectiveness for minimizing data failure and maximizing throughput.

Reddy et al.[14] proposed a reliable multi-path routing protocol for MANETs in urban areas. The protocol was designed to be based on link quality and stability which aimed to address challenges of communication in a dynamic and unpredictable environment. In their research, the authors highlighted the vulnerability of MANETs to denial-of-service attacks, blackhole attack which could result in a total data loss. To address this issue, the author proposed the integration of the various protocols with some built-in security features. The paper evaluated the performance of blackhole attack and the proposed AODV-BS protocol on MANET models based on network metrics such as network PDR, normalized routing overhead utilization, and network delay. The proposed protocol showed promising results by improving network reliability and security.

Benatia et al.[15] focuses on developing a reliable routing protocol for MANETs in urban areas. Several routing protocols have been discussed for MANETs, such as AODV, DSR. However, these protocols have limitations in terms of reliability, scalability, and performance, especially in urban environments, where the presence of buildings and other obstacles can cause signal attenuation, interference, and link instability. To address these issues, the author proposed ELE-AOMDV protocol based on link quality and stability metrics. The protocol gathered information from neighboring nodes and the link quality metric, while the stability metric is based on the link duration and the total packet lost. ELE-AOMDV also employs a path switching mechanism to switch to a more reliable path in case of link failure or congestion. Results indicate that proposed protocol outperforms in terms of PDR, end-to-end delay, and throughput, especially in urban environments with high node densities and mobility.

In conclusion, the reviewed studies suggest that ML techniques and deep learning approaches can enhance the efficiency of routing protocols in MANETs. These techniques have demonstrated excellent results in

detecting attacks and improving network efficiency. Future research could focus on exploring the effectiveness of combining these techniques to further improve network security and efficiency.

3. Problem formulation

The aim of research is to propose a innovative K-AOMDV or efficient data routing in MANET. Black hole attack in AOMDV routing protocol is a very common problem due to which the efficiency decreases as drop packets get increases and malicious nodes makes the route discovery formation complex which leads to multiple packet failure and decreased throughput. To avoid falsely claimed route and determining the optimal next step fuzzy models would be beneficial. The proposed method utilizes K-means clustering, reinforcement learning, and a fuzzy model to determine the least-parametrically-intensive solution to a problem explained in section 3. The AOMDV protocol can eliminate routing loops because it ensures that the order of the destinations on a valid route always increases as they get closer to the destination. It has been suggested that a clustering-based AOMDV protocol might address this problem by selecting routes when the original protocol, which does not consider energy constraints, is ineffective. Using the distance vector concept, AOMDV takes a hop-by-hop method to route.

The issue of malicious node continuously decreasing performance of protocol, proposed method contains the deployment of sensor nodes randomly to collect data, which generates frame clusters. The performance metrics includes throughput, packet delivery rate, normalized routing overload and normalized energy consumption. K-means clustering method is initiated to form clusters of nodes with similar characteristics, selecting the best-optimized node as the node head, and optimizing the distances between the node head and other nodes in the cluster. The proposed protocol continues to broadcast if an attack is detected during transmission using a new route and utilizes the existing way if no attack is detected. Performance metrics for this phase include the throughput, packet delivery rate, normalized routing overload, and normalized energy consumption. The performance of proposed K-AOMDV is analyzed using support vector machine (SVM) for system training and testing. The evaluation criteria include accuracy, precision, F1-Score, and recall. The study aims to improve the performance of MANET by optimizing data route and addressing against black hole attacks using Machine learning techniques.

4. Research objectives

The following are some of the goals that the study hopes to achieve:

- To develop a MANET routing protocol suitable for the challenging environment to ensure effective routing.
- This study determines whether the K-AOMDV routing protocol is effective in terms of the packet delivery ratio, throughput, and energy consumption after it has been normalized; the objective is to investigate how well it would allow one to evaluate the efficiency of the protocol.
- To conduct research and an assessment of the efficiency of the K-AOMDV routing protocol both with and without a blackhole assault.
- To assess how well the K-AOMDV routing protocol utilizes the SVM classifier.

5. Research methodology

The research methodology involves three phases for designing a novel routing protocol called K-AOMDV. In Phase I, sensor nodes are randomly deployed to collect data, and frame clusters are generated. The number of nodes for throughput, packet delivery rate, normalized routing overload, and energy consumption are calculated and visualized. Phase II involves forming clusters of nodes using K-means clustering, where nodes with the same characteristics are grouped together, and the best-optimized node

becomes the node head. In Phase III, the transition probability of the network is calculated, and clustering is done using a fuzzy model for optimum route installation. A blackhole attack is used for attack detection and transmission, and K-AOMDV is calculated with and without blackhole attacks. Support Vector Machines (SVM) is used for system training and testing, and the best accuracy, precision, F1-score, recall is calculated.

In this research, various methods will be explored including fuzzy modeling, K-means clustering, black hole attacks, SVM. They will be used to increases the K-AOMDV routing protocol and improve its performance are addressed below:

5.1. Fuzzy model

Fuzzification is a fundamental component of Fuzzy Logic Systems. The membership functions, which motivate both the rule-based inference and defuzzification procedures, represent human interpretation using a mathematical approach known as fuzzing[16]. There are many membership functions available, including those based on geometric shapes and plausibility of event occurrence or language expression, such as the triangle, trapezoidal, sigmoid, and Gaussian functions. All linguistic variables have membership functions generated for them, which can be based on the knowledge of specialists or data gathered from studies. Fuzzy patches can be used to determine the portion of a fuzzy rule that is produced consequently when the system's response is already known. The fuzzy inference mechanism decides how fuzzy rules for antecedent values should be performed, and the result is a fuzzy conclusion[17]. **Figure 1** depicts the fuzzy logic control system.

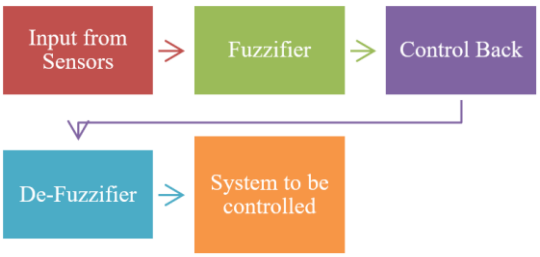

Figure 1. A fuzzy logic control system[18].

5.1.1. K-mean clustering

The K-means clustering method is prominently used for vector quantization and originated in signal processing. Its primary aim is to group n observations into k clusters, with each cluster having an average value as close as possible to the observations assigned to it. The K-means algorithm is commonly works after the data space has been partitioned into node-link cells in previous stages of processing. The average is the only statistic that can reduce the mean square error, while the geometric median is the only statistic that can eliminate Euclidean distances[19].

5.1.2. Blackhole attack

Black hole attacks occur when a router fails to deliver messages correctly and instead deletes them.As shown in **Figure 2** in some cases, the router's configuration can become so corrupt that it provides a path to any destination on the Internet at no additional cost. This can happen if the router's firmware becomes corrupted. If an attacker were to take advantage of this, the result would be that the router would receive all of the traffic. However, the router would fail since there is no other device that could sustain such a load at the same time. An attack is carried out by an attacker who seizes and reprograms a set of network nodes to either block or delete packets and produce fake signals instead of sending correct or actual information to the base station located in a black hole.

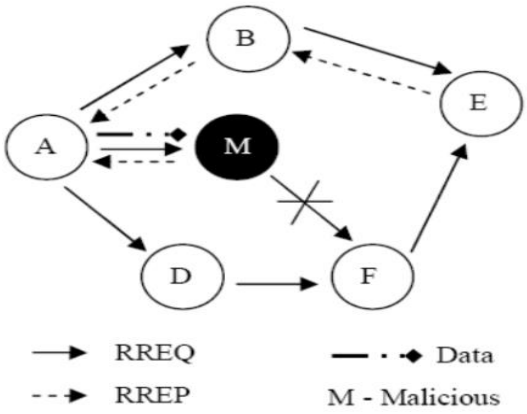

Figure 2. Black hole attack in AOMDV[20].

5.1.3. Support vector machine (SVM)

SVM is ML algorithm used for system training and testing for evaluating the efficiency of K-AOMDV. Also it is used for classification and regression analysis. In the context of K-AOMDV, SVM can be used to train the system on a set of input-output pairs and learn the optimal decision boundaries that separate different classes of data. Once the system is trained, it can be tested on a separate set of data to evaluate its performance. By using SVM for system training and testing, K-AOMDV can be optimized for performance and accuracy in detecting and preventing black hole attacks. **Figure 3** depicts the SVM that was built using ML.

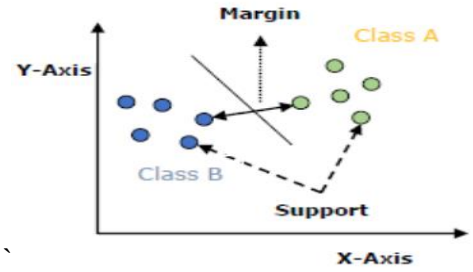

Figure 3. SVM using ML[15].

Developing effective routing algorithms for wireless mesh networks can be challenging due to the dynamic nature of network design. Such algorithms need to quickly and efficiently locate new routes through the network nodes.

6. Proposed methodology

Several phases of the suggested technique will be covered in the following section of this paper. The flow chart of the anticipated technique for preprocessing the information obtained from black hole assaults is shown in **Figure 4**. If an attack is discovered, the communication will be rerouted to a new path; if no assault is found, the communication will proceed in the same way as before. Distribution of networks in clusters below.

Motivation behind proposed routing protocol

The proposed routing protocol aims to discover a loop free and disjoint method for communication for optimizing the performance of protocol. To achieve this motive KNN is being used for examining the optimality by creating clusters of similar nodes which makes the route discovery easier by reducing the mean square error rate. Being the hop-by-hop routing protocol (AOMDV), the intermediate node can maintain multiple path entries in their respective routing table and to discover distinct paths, K-AOMDV suppresses duplicate RREQs at intermediate nodes. Also SVM technique is used to investigate the performance of proposed protocol on parameter shown in results section.

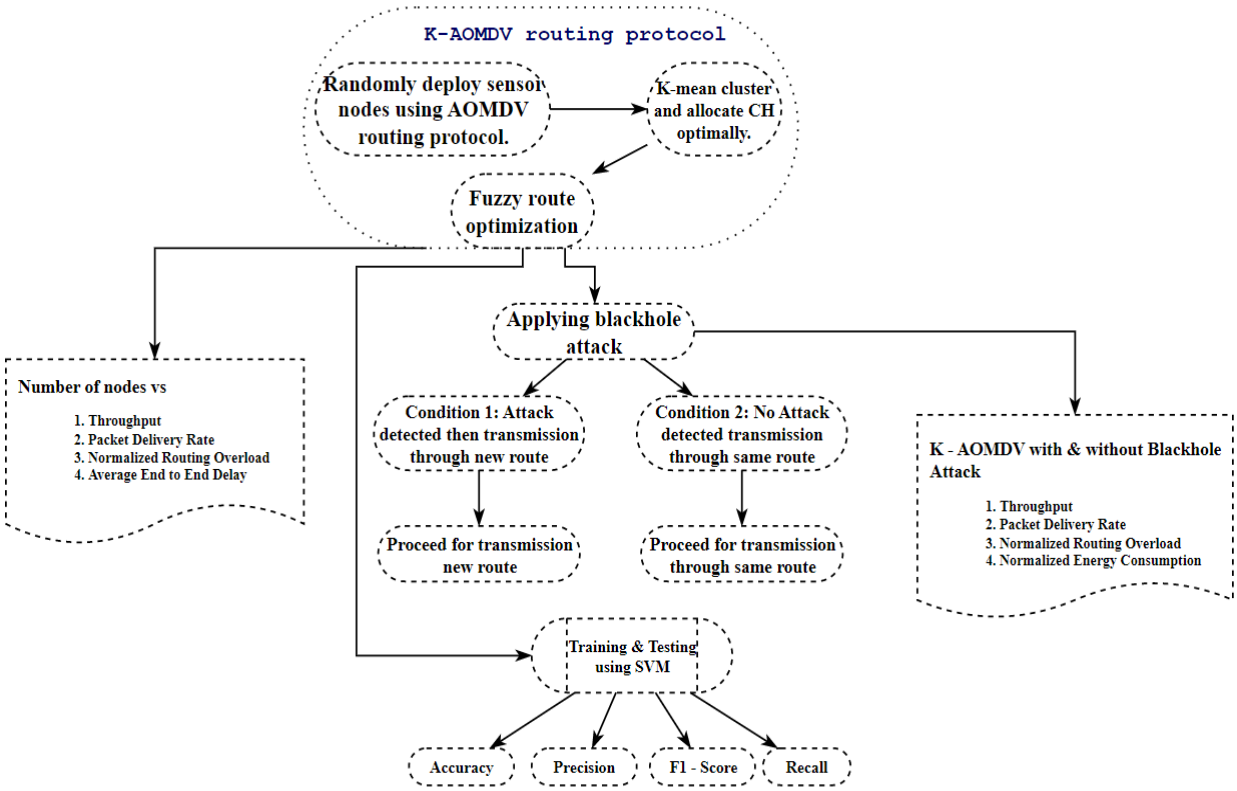

Figure 4. Proposed methodology.

7. Proposed algorithm

The proposed algorithm is to design K—AOMDV Routing Protocol.

Algorithm K-AOMDV Routing Protocol Algorithm

Phase I: Design K-AOMDV Routing Protocol
Step 1: K-AOMDV Routing deploys sensor nodes randomly to collect data.
Step 2: This data generates frame clusters.
Phase II: Calculation of distances b/w node head and other nodes using K-AOMDV
Step 3: K-means clustering is used to form clusters of nodes.
Step 4: Nodes with the same characteristics should form clusters.
Step 5: The best-optimized node will be the node head.
Step 6: The distances between Node Head and other nodes will be optimal for each cluster.
Phase III: To simulate the number of nodes using NS3 simulator for investigation of network performance parameters
Step 7: Clustering for selected optimum route installations using a fuzzy model.
Step 8: Then a blackhole attack is used for attack detection and transmission.
Step 9: If an attack is detected during transmission using a new route, continue to broadcast; if no attack is detected, continue utilizing the existing way.
Step 10: Using K-AOMDV with and without blackhole attacks analysing the parameter such as. Throughput, Packet Delivery rate, Normalized Routing Overload, Normalized energy consumption.
Step 11: Now, SVM is being utilized for system training and testing in comparing and grouping each set of networks for the calculation of following parameters such as Accuracy, Precision, F1-Score, Recall

Performance network metrics

Energy Efficiency: It is the requirements in order to save precious energy of the sensor nodes resulting in extended lifetime of the network. Routing protocols for delay sensitive applications tend to reduce the number of transmissions in order to save energy.

Throughput: Rate of successful message delivery over a communication channel.

Packet Delivery Ratio: Ratio of number of packets received at the destination to the number of packets sent from the source. The performance is better when packet delivery ratio is high.

End to End Delay: Time taken for a packet to be transmitted across a network from source to destination.

Routing Overhead: Number of routing packets required for network communication.

Precision score: In machine learning it measures the proportion of positively predicted labels that are actually correct.

Recall score: The model's ability to correctly predict the positives out of actual positives.

Accuracy score: Ratio of true positives and true negatives to all positive and negative observations.

8. Results analysis

Table of simulation

The simulation was conducted with 100 nodes and a simulation time of 900 seconds. The Random Direction mobility model with a maximum speed of 10 m/s and pause times ranging from 0 to 900 seconds in increments of 60 seconds. The communicating nodes varied from 10 to 100. The application layer used Constant Bit Rate and the routing protocol employed was K-AOMDV. These parameters that are presented in **Table 1** were carefully selected to simulate a realistic wireless mesh network environment, where nodes move randomly, communicate with varying numbers of neighbors, and use a constant bit rate application. The K-AOMDV protocol was used for evaluation under these conditions and determines its effectiveness in ensuring reliable data transmission and reducing the impact of network disruptions.

Table 1. Table of simulation.

Simulation Parameters	Value
No. of nodes	100
Simulation time (s)	900
Mobility Model	Random Direction (RD)
Maximum speed (m/s)	10 sec
Pause time (s)	60, 120, 180, 240, 300, 360, 420, 480, 540, 600, 660, 720, 780, 840, 900
No. of communicating nodes	10, 20, 30, 40, 50, 60, 70, 80, 90, 100
Application layer	Constant Bit Rate
Routing protocols	K-AOMDV

- **Throughput vs. node:**

Figure 5 shows the performance of protocols such as AODV[14], K-AOMDV, AODV-BS with blackhole[14] and K-AOMDV with blackhole, under different network scenarios in terms of throughput vs number of nodes. The results show that K-AOMDV generally performs better than AODV w.r.t. throughput, especially for networks with a smaller number of nodes. However, the study highlights that both protocols experience a significant drop in throughput when a blackhole attack is introduced, and K-AOMDV with and without blackhole attacks performs better than AODV and AODV-BS with blackhole in terms of PDR and throughput.

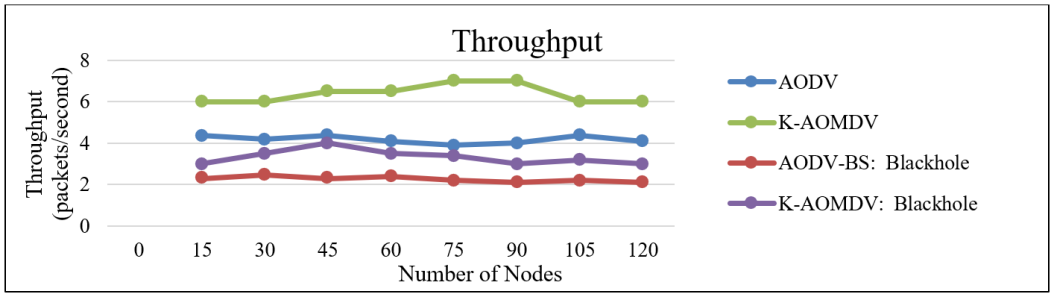

Figure 5. Throughput vs. Number of Nodes: K-AOMDV with and without Blackhole attack.

- **Packet delivery ratio (PDR)**

The **Figure 6**, where the Packet Delivery Ratio (PDR) vs. Number of Nodes for different routing protocols is presented, compares the performance of different routing protocols, including AODV[14], K-AOMDV, AODV-BS with blackhole[14] and K-AOMDV with blackhole. The comparison indicates that K-AOMDV with and without blackhole attacks provides better packet delivery rates than AODV and AODV-BS with blackhole. These findings highlight the importance of choosing an effective routing protocol and implementing security measures to ensure reliable and secure data transmission in wireless networks.

$$PDR = \frac{Packets\ received}{Packets\ sent} \times 100 \tag{1}$$

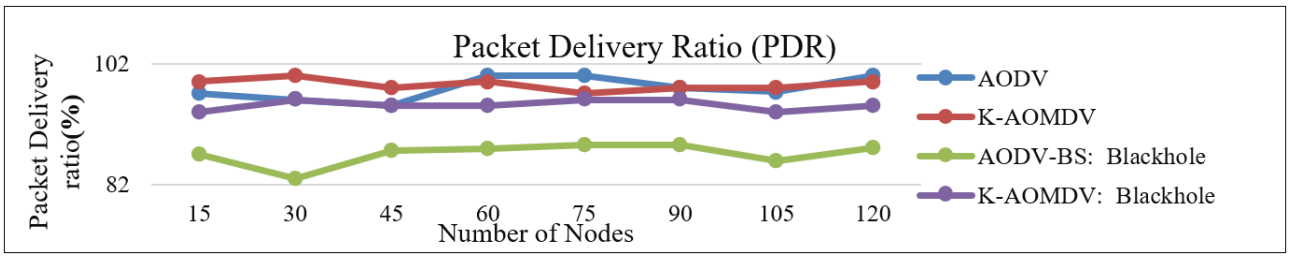

Figure 6. Packet delivery ratio vs. amount of nodes.

- **Average end-to-end delay**

The performance of different routing protocols w.r.t. AEED is compared in **Figure 7** and the results shows that K-AOMDV generally outperforms AODV[13]. The study emphasizes the significance of selecting an efficient routing protocol and implementing security measures to minimize adverse effects of malicious attacks on network and ensure reliable data transmission from 0 to 15 nodes all protocols having equal AEED except AODV-Bs while during transition from 30 to 120 K-AOMDV performs nearly better after blackhole attack w.r.t. to other comparative protocols.

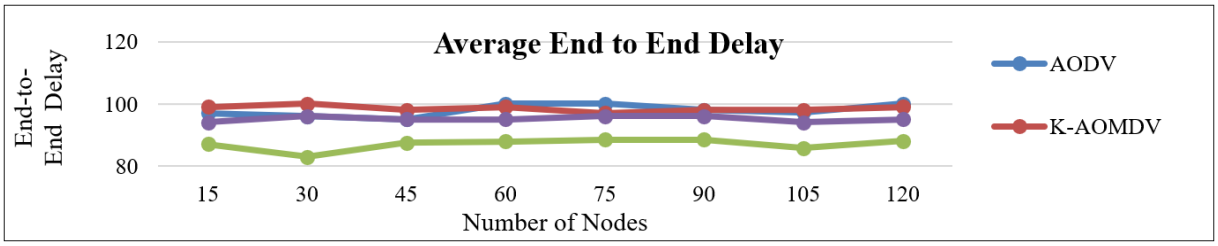

Figure 7. Average end-to-end delay vs. no. of nodes.

- **Normalized energy consumption**

The total of all nodes' simulation energy over the ratio of received data packets. The normalized energy consumption of connection l over Δ_l Is:

$$\frac{(Initial\ Energy - Residual\ Energy)}{Received\ data\ packet\ ratio} \tag{2}$$

Figure 8, compares the performance of different routing protocols, including AODV[14], K-AOMDV, AODV-BS with blackhole[14], and K-AOMDV with blackhole. The comparison takes into account the routing overhead and the no. of control packets generated by the protocols. The results indicate that K-AOMDV has a lower normalized routing overload than AODV in all scenarios, indicating that K-AOMDV generates fewer control packets and is less likely to overload the network with routing messages. Moreover, the comparison indicates that introducing a blackhole attack increases the normalized routing overload for all protocols, with

AODV-BS with blackhole and K-AOMDV with blackhole being the most affected. The findings suggest that K-AOMDV is a more efficient routing protocol in terms of routing overhead, especially during blackhole attack. The results highlighted the importance of selecting a routing protocol that can provide reliable and efficient routing while minimizing the routing overhead in wireless networks.

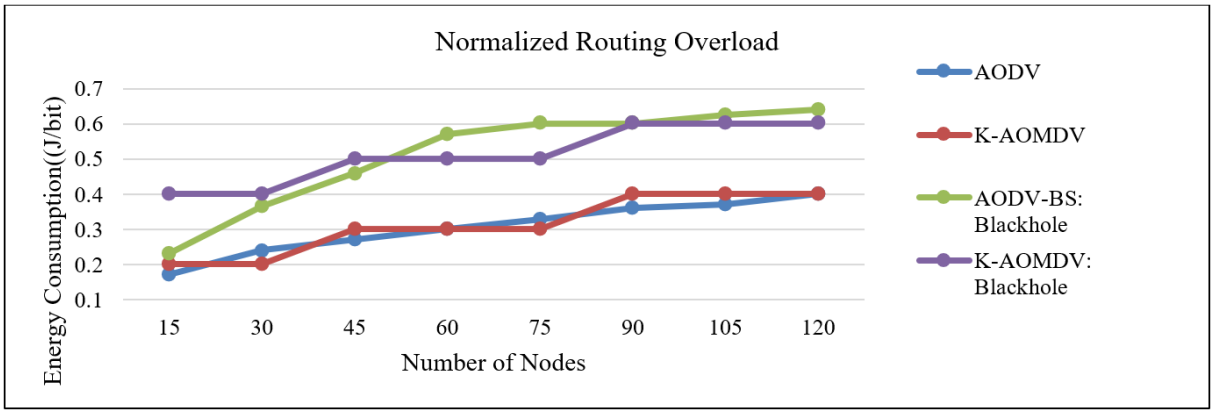

Figure 8. Normalize energy consumption vs. number of nodes: K-AOMDV with and without blackhole attack.

Table 2 shows that K-AOMDV with blackhole shows better results w.r.t. PDR and overhead compared to the other two protocols, while ELE-AOMDV[15] has the highest throughput and normalized energy consumption. The table provides insights into the performance trade-offs for various networks.

Table 2. Comparison analysis.

No. of Nodes	PDR			Overhead			Throughput			Normalized Energy Consumption		
	ELE-AOMDV [15]	K-AOMDV	K-AOMDV: Blackhole	ELE-AOMDV [15]	K-AOMDV	K-AOMDV: Blackhole	ELE-AOMDV [15]	K-AOMDV	K-AOMDV: Blackhole	ELE-AOMDV [15]	K-AOMDV	K-AOMDV: Blackhole
10	55	70	59	0	2	3	12	15	11	2	3.5	6
20	60	74	68	1	1	2	12.3	14	9	5	3	6
30	62	72	68	1	3	4	12.5	17	14	6	4.45	7
40	65	80	73	2	2	6	13	20	15	7	5.24	7
50	68	85	75	4	5	8	13.7	22	15	9	5	7
60	70	84	74	7	4	7	14	21	16	16	6.75	8
70	72	88	76	10	6	8	14.2	23	14	16	6.44	10
80	74	90	75	13	5	10	14.7	25	17	18	8.5	9
90	76	92	82	15	7	9	15	24	19	20	8	11
100	77	95	85	20	10	12	15.5	28	20	22	9	11

- **Throughput**

Figure 9 illustrates the comparison of the throughput performance of different routing protocols, including ELE-AOMDV[15], K-AOMDV, and K-AOMDV with blackhole attacks under different network scenarios based on the no. of nodes. Results depicts that as the nodes increases, K-AOMDV's performance drops slightly and when a blackhole attack is introduced, the throughput of K-AOMDV decreases significantly, and the comparison indicates that K-AOMDV with blackhole attacks provides lower throughput than K-AOMDV without blackhole attacks. The results also highlight the importance of implementing security measures to protect the network from malicious attacks that may impact its performance.

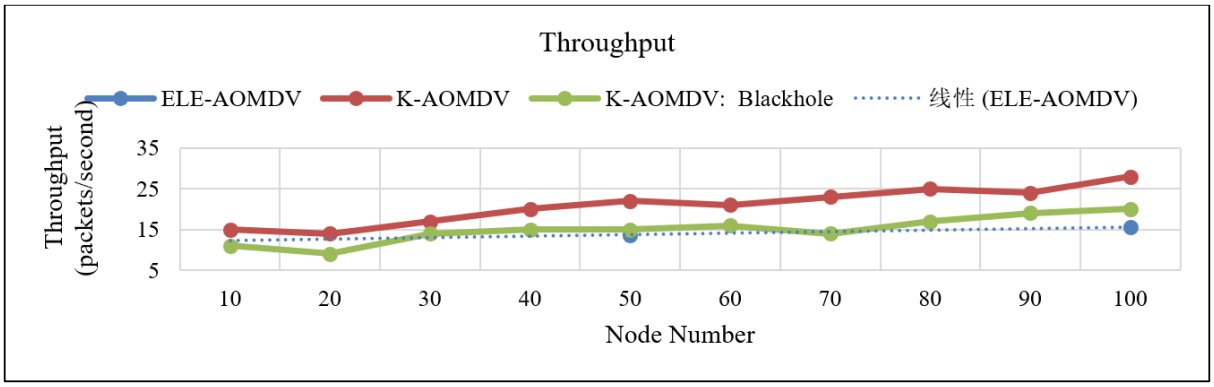

Figure 9. Throughput vs. number of nodes for ELE-AOMDV[15], K-AOMDV and K-AOMDV-blackhole.

- **Packet delivery rate vs. node**

PDR is an essential metric to evaluate the effectiveness of routing protocols in wireless networks. **Figure 10** shows that K-AOMDV with and without blackhole attacks generally provides better PDR than ELE-AOMDV. During 10–40 nodes they are continuously delivering the packets whereas as the nodes increases K-AOMDV without blackhole attacks exhibits a similar PDR to K-AOMDV with blackhole attacks in larger networks. These findings suggest that K-AOMDV is a promising routing protocol for wireless networks that provides high PDR and reliable data transmission, even under malicious attacks as the nodes increase.

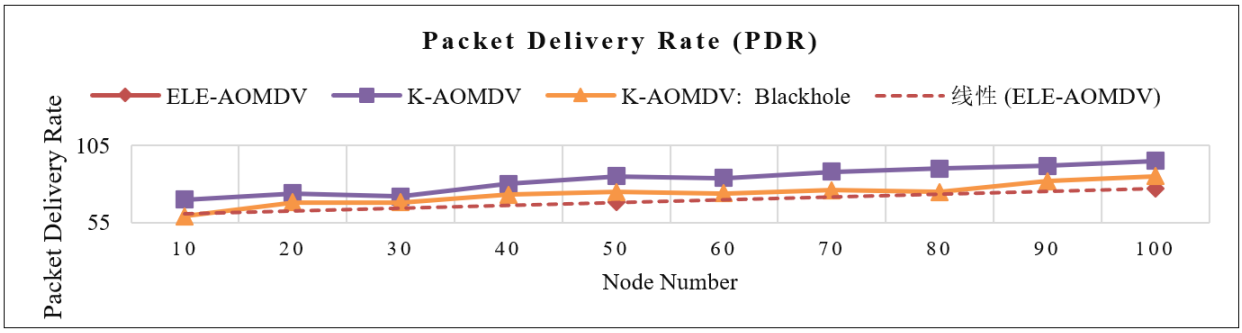

Figure 10. Packet delivery rate vs. number of nodes for ELE-AOMDV[15], K-AOMDV and K-AOMDV- blackhole.

- **Overhead rate vs. node**

The overhead is measured as the control messages exchanged between nodes during its routing process. The results show ELE-AOMDV has the lowest overhead than K-AOMDV with blackhole. In contrast, K-AOMDV's overhead increases with the increased nodes, but it is still less than K-AOMDV with blackhole. These findings demonstrate that ELE-AOMDV is a more efficient routing protocol in terms of overhead compared to K-AOMDV and K-AOMDV with blackhole, and it could be an appropriate choice for networks where the number of nodes is small as shown in **Figure 11**.

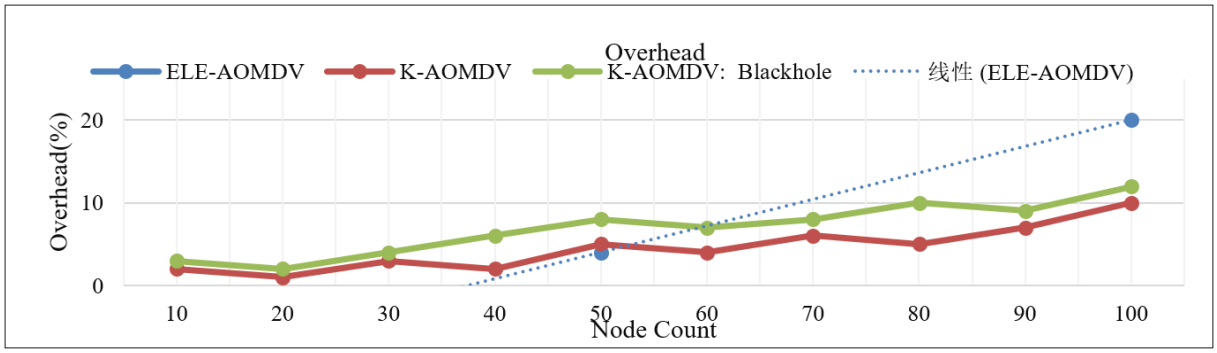

Figure 11. Overhead vs. number of nodes for ELE-AOMDV[15], K-AOMDV and K-AOMDV- blackhole.

- **Normalized energy consumption vs. node speed**

Normalized Energy Consumption plays major metric for observing the efficiency of wireless networks. **Figure 12** provides the comparison of Normalized Energy Consumption for ELE-AOMDV[15], K-AOMDV, and K-AOMDV with blackhole attack. The results depicts that the K-AOMDV is far better and as the number of nodes increases energy consumption is way too much for ELE-AOMDV[15]. Overall, the findings show that K-AOMDV with blackhole attack is the most energy-efficient routing protocol among the three, and it can be an excellent choice for wireless networks that require energy-efficient communication.

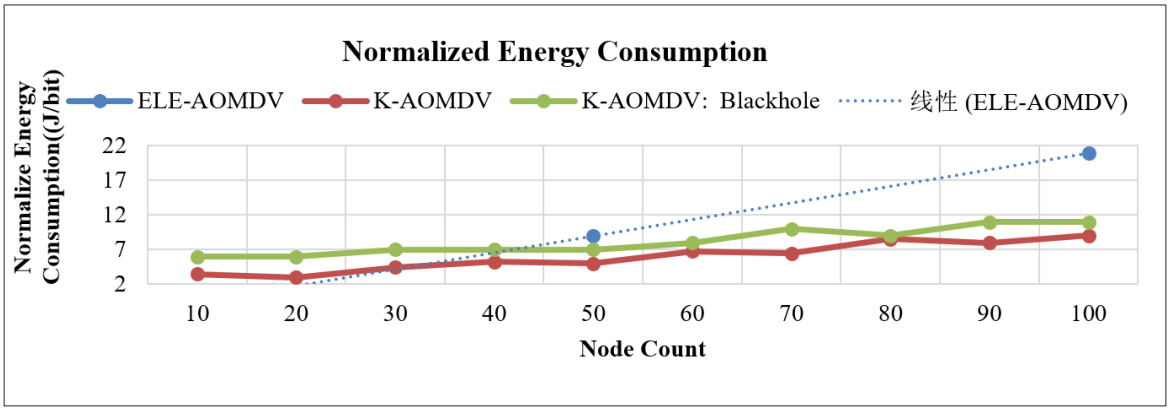

Figure 12. Normalize Energy Consumption((J/bit) vs. Number of Nodes: 10 to 100 points updated with valuation and ELE-AOMDV with existed value.

9. Classification report

According to the classification report presented in **Table 3** and **Figure 13** the performance of K-AOMDV routing protocol using SVM, the model has gain accuracy of 0.99% and a cross-validated Receiver Operating Characteristic (ROC) with A.U.C. which is a commonly used metric to assess the thoroughly performance of a binary classification model. The K-AOMDV algorithm has achieved an AUC of 0.009% error with the Support Vector Machine algorithm which depicts by higher the AUC value more the better performance ranges between 0 to 1.

Table 3. Classification report of K-AOMDV routing protocol.

	Precision	Recall	f1-score	SVM
0	0.80	1.00	0.89	8
1	1.00	0.99	0.99	196
accuracy			0.99	204
macro avg	0.90	0.99	0.94	204
Weighted avg	0.99	0.99	0.99	204

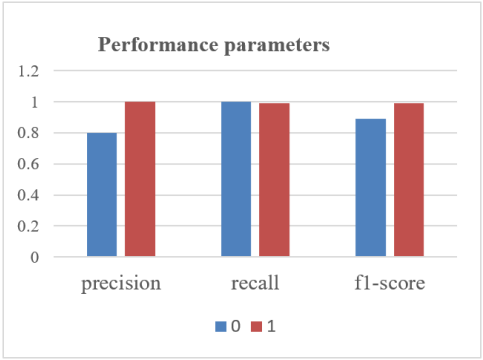

Figure 13. Performance of K-AOMDV routing protocol.

10. Conclusion and future scope

Study concludes to develop and evaluate the K-AOMDV routing protocol for MANETs in challenging environments. The study presents a simulation-based evaluation of the performance of the K-AOMDV in a wireless mesh network environment. The simulation was conducted with 100 nodes and a simulation time of 900 seconds, using the Random Direction mobility model, Constant Bit Rate (CBR) application layer, and communicating nodes. The simulation results indicated that K-AOMDV generally outperforms in terms of throughput, PDR, Average End-to-End Delay and normalized energy consumption, especially for networks with a smaller number of nodes. The study also highlighted importance of implementing security measures to lessen the effect of malicious attacks on network performance. The findings of this study provide insights into the effectiveness of the K-AOMDV routing protocol in a wireless mesh network environment. Future research could explore the performance of other routing protocols under similar network conditions and compare their performance with that of K-AOMDV. Further research could be extended to investigate the impact various types of attacks, such as wormhole, Sybil attacks and many more on network performance and evaluate the effectiveness of different security measures in mitigating these attacks. Overall, the K-AOMDV protocol provides a promising direction for future research in secure MANET's Routing.

Author contributions

Conceptualization, SK and KT; methodology, SK; software, SK and PM; validation, SK, KT and PM; formal analysis, SK; investigation, SK; resources, SK; data curation, SK; writing—original draft preparation, SK; writing—review and editing, SK, KT, RG and PM; visualization, SK and KT; supervision, PM and KT; project administration, SK; funding acquisition, RG and PM. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. S. Raj J. Machine Learning Based Resourceful Clustering With Load Optimization for Wireless Sensor Networks. 2020, 2(1): 29-38. doi: 10.36548/jucct.2020.1.004
2. Yasin A, Abu Zant M. Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique. Wireless Communications and Mobile Computing. 2018, 2018: 1-10. doi: 10.1155/2018/9812135
3. Hossain S, Hussain MdS, Ema RR, et al. Detecting Black hole attack by selecting appropriate routes for authentic message passing using SHA-3 and Diffie-Hellman algorithm in AODV and AOMDV routing protocols in MANET. 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). 2019. doi: 10.1109/icccnt45670.2019.8944395
4. Tami A, Boukli Hacene S, Ali Cherif M. Detection and Prevention of Blackhole Attack in the AOMDV Routing Protocol. Journal of Communications Software and Systems. 2021, 17(1): 1-12. doi: 10.24138/jcomss.v17i1.945
5. Bhardwaj AK. Machine Learning based Power Efficient Optimized Communication Ensemble Model with Intelligent Fog Computing for W.S.N.s. 2022.
6. Abdan M, Seno SAH. Machine Learning Methods for Intrusive Detection of Wormhole Attack in Mobile Ad Hoc Network (MANET). Wireless Communications and Mobile Computing. 2022, 2022: 1-12. doi: 10.1155/2022/2375702
7. Sivanesan N, Archana KS. A machine learning approach to detect network layer attacks in mobile ad hoc networks. International Journal of Early Childhood. 2022, 14(3).
8. Alsarhan A, Alauthman M, Alshdaifat E, et al. Machine Learning-driven optimization for SVM-based intrusion detection system in vehicular ad hoc networks. Journal of Ambient Intelligence and Humanized Computing. 2021, 14(5): 6113-6122. doi: 10.1007/s12652-021-02963-x
9. Rajendran A, Balakrishnan N, P A. Deep embedded median clustering for routing misbehaviour and attacks detection in ad-hoc networks. Ad Hoc Networks. 2022, 126: 102757. doi: 10.1016/j.adhoc.2021.102757
10. Chen L, Hu B, Guan ZH, et al. Multiagent Meta-Reinforcement Learning for Adaptive Multipath Routing Optimization. IEEE Transactions on Neural Networks and Learning Systems. 2022, 33(10): 5374-5386. doi: 10.1109/tnnls.2021.3070584

11. Guo W, Yan C, Lu T. Optimizing the lifetime of wireless sensor networks via reinforcement-learning-based routing. International Journal of Distributed Sensor Networks. 2019, 15(2): 155014771983354. doi: 10.1177/1550147719833541
12. Kaushik S, Tripathi K, Gupta R, et al. Performance Analysis of AODV and SAODV Routing Protocol using SVM against Black Hole Attack. 2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM). 2022. doi: 10.1109/iciptm54933.2022.9754166
13. Kaushik S, Tripathi K, Gupta R, et al. Futuristic Analysis of Machine Learning Based Routing Protocols in Wireless Ad Hoc Networks. 2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT). 2021. doi: 10.1109/ccict53244.2021.00067
14. B PR, B BR, B D. The AODV routing protocol with built-in security to counter blackhole attack in MANET. Materials Today: Proceedings. 2022, 50: 1152-1158. doi: 10.1016/j.matpr.2021.08.039
15. Benatia SE, Smail O, Meftah B, et al. A reliable multipath routing protocol based on link quality and stability for MANETs in urban areas. Simulation Modelling Practice and Theory. 2021, 113: 102397. doi: 10.1016/j.simpat.2021.102397
16. Bhole K, Agashe S, Wadgaonkar J. How Expert is EXPERT for Fuzzy Logic-Based System! International Proceedings on Advances in Soft Computing, Intelligent Systems and Applications. 2017: 29-36. doi: 10.1007/978-981-10-5272-9_3
17. Mirza S, Gujarathi T, Bhole K. Cardiovascular Risk Assessment Using Intuitionistic Fuzzy Logic System. 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). 2019. doi: 10.1109/icccnt45670.2019.8944853
18. Rad D, Rad G, Maier R, et al. A fuzzy logic modelling approach on psychological data. Journal of Intelligent & Fuzzy Systems. 2022, 43(2): 1727-1737. doi: 10.3233/jifs-219274
19. Michael J, Garbade J. Understanding k-means clustering in machine learning. 2019.
20. Khan M, Khaeel U, Ramesh KS. Effect on Packet Delivery Ratio (PDR) & Throughput in Wireless Sensor Networks Due to Black Hole Attack. Int. J. Innov. Technol. Explor. 2019, 8(12S): 428-432. doi: 10.35940/ijitee.l1107.10812s19